A quantitative Khintchine–Groshev type theorem over a field of formal series

M. M. Dodson[1], S. Kristensen[2] and J. Levesley[3]

[1]Department of Mathematics, University of York,
Heslington, York, YO10 5DD, UK
mmd1@york.ac.uk

[2]School of Mathematics, University of Edinburgh, JCMB,
King's Buildings, Mayfield Road, Edinburgh, EH9 3JZ, UK
Simon.Kristensen@ed.ac.uk

[3]Department of Mathematics, University of York,
Heslington, York, YO10 5DD, UK
jl107@york.ac.uk

February 1, 2008

Abstract

An asymptotic formula which holds almost everywhere is obtained for the number of solutions to the Diophantine inequalities $\|\mathbf{q}A - \mathbf{p}\| < \psi(\|\mathbf{q}\|)$, where A is an $n \times m$ matrix ($m > 1$) over the field of formal Laurent series with coefficients from a finite field, and $\mathbf{p}$ and $\mathbf{q}$ are vectors of polynomials over the same finite field.

AMS Subject Classification: 11J83, 11J61

Key Words and Phrases: Diophantine approximation, positive characteristic, systems of linear forms, asymptotic formulae.

1 Introduction

Let $\mathbb{F}$ denote the finite field of $k = p^l$ elements, where p is a prime and l is a positive integer. We define

$$\mathcal{L} = \left\{ \sum_{i=-n}^{\infty} a_{-i} X^{-i} : n \in \mathbb{Z}, a_i \in \mathbb{F}, a_n \neq 0 \right\} \cup \{0\}. \tag{1}$$

Under usual addition and multiplication, this set is a field, sometimes called *the field of formal Laurent series with coefficients from* $\mathbb{F}$. We may define an absolute value on $\mathcal{L}$ by setting

$$\left\| \sum_{i=-n}^{\infty} a_{-i} X^{-i} \right\| = k^n, \quad \|0\| = 0.$$

This absolute value is ultra-metric. Under the induced metric, $d(x, y) = \|x - y\|$, the space $(\mathcal{L}, d)$ is a complete metric space.

The approximation of elements of $\mathcal{L}$ by ratios of elements in the polynomial ring $\mathbb{F}[X]$ has been studied extensively (see *e.g.* the survey papers by Lasjaunias [4] and Schmidt [9]) and has been used in the analysis of pseudorandom sequences employed in cryptography by Niederreiter and Vielhaber [6].

In this paper, we are concerned with the metrical theory of such Diophantine approximations. Let $\psi : \mathbb{R}_+ \to \mathbb{R}_+$ be a function with $\psi(x)$ non-increasing. In [1], de Mathan showed that the set of elements $x \in \mathcal{L}$ for which the inequality

$$\|qx - p\| < \psi(\|q\|)$$

has infinitely many solutions $q, p \in \mathbb{F}[X]$, $q \neq 0$ is null or full (with respect to the Haar measure) accordingly as the series $\sum_{r=1}^{\infty} \psi(r)$ diverges or converges. This was extended to systems of linear forms in Kristensen [3], as follows.

Theorem 1 ([3, Theorem 3]). *Let $\psi : \mathbb{R}_+ \to \mathbb{R}_+$ be decreasing. Let $m, n \in \mathbb{N}, m \geq 2$. The set of $m \times n$ matrices A with entries from $\mathcal{L}$ for which the inequalities*

$$\|\mathbf{q}A - \mathbf{p}\|_\infty < \psi(\|\mathbf{q}\|_\infty) \tag{2}$$

have infinitely many solutions $\mathbf{p} \in \mathbb{F}[X]^n$, $\mathbf{q} \in \mathbb{F}[X]^m, \mathbf{q} \neq \mathbf{0}$ is null or full accordingly as the series $\sum_{r=1}^{\infty} r^{m-1}\psi(r)^n$ converges or diverges, where $\|\mathbf{q}\|_\infty = \max\{\|q_i\|\}$ for $\mathbf{q} = (q_1, \dots, q_m)$.

Here, we are concerned with the asymptotic number of solutions to the inequalities (2). In the real case, the analogous asymptotics were found by Schmidt, first in the case of simultaneous approximation as well as approximation of a single linear form in Schmidt [7] and since for systems of linear forms as well as for restricted sets of $\mathbf{q}$'s in Schmidt [8].

We will restrict ourselves to considering error functions taking their values in the set $V = \{k^{-n} : n \in \mathbb{N}\}$. For general error functions, see the remark following the statement of the theorem. We will prove the following theorem:

Theorem 2. *Let $\epsilon > 0$, let $\psi : \mathbb{R}_+ \to V$ and let $N(Q,A)$ denote the number of solutions to (2) with $\|\mathbf{q}\|_\infty \leq k^Q$. Let*

$$\Phi(Q) = m(k-1)k^{m-1}\sum_{r=0}^{Q} k^{rm}\psi(k^r)^n$$

Then

$$N(Q,A) = \Phi(Q) + O\left(\Phi(Q)^{1/2}\log^{3/2+\epsilon}(\Phi(Q))\right)$$

for almost every $m \times n$ matrix A with entries from $\mathcal{L}$.

The reason for restricting the choice of error functions is that the only possible distances in the space $\mathcal{L}$ are of the form k^r where $r \in \mathbb{Z}$. For other error functions, we could define a function, $\lfloor\cdot\rfloor : \mathbb{R}_+ \to V$ say, mapping $x \in \mathbb{R}$ to the unique number $\lfloor x\rfloor \in V$ such that $\lfloor x\rfloor \leq x < k\lfloor x\rfloor$. On replacing $\psi(\cdot)$ with $\lfloor\psi(\cdot)\rfloor$ at every occurence, we would obtain the theorem for general decreasing error functions. However, for ease of notation we consider only the restricted case.

2 Proof of main theorem

The proof has two main ingredients. The first has to do with the geometry of the underlying vector spaces. The second is a purely probabilistic theorem. We first prove the geometrical results.

We identify $\mathrm{Mat}_{m\times n}(\mathcal{L})$ with $\mathcal{L}^{mn}$. Define for any $\mathbf{q} \in \mathbb{F}[X]^m$ the set

$$B_{\mathbf{q}} = \left\{A \in I^{mn} : \inf_{\mathbf{p}\in\mathbb{F}[X]^n} \|\mathbf{q}A - \mathbf{p}\|_\infty < \psi(\|\mathbf{q}\|_\infty)\right\}, \tag{3}$$

where I^{mn} denotes the $\|\cdot\|_\infty$-unit ball in $\mathcal{L}^{mn}$. The Haar measure on $\mathcal{L}^{mn}$, normalised so that the measure of I^{mn} is equal to 1, will be denoted by μ.

We will prove the following propositions:

Proposition 3.

$$\mu\left(B_{\mathbf{q}}\right)) = \psi(\|\mathbf{q}\|_{\infty})^n.$$

Proposition 4. *Let* $\mathbf{q}, \mathbf{q}' \in \mathbb{F}[X]^m$ *be linearly independent over* $\mathcal{L}$*. Then*

$$\mu\left(B_{\mathbf{q}} \cap B_{\mathbf{q}'}\right) = \mu\left(B_{\mathbf{q}}\right)\mu\left(B_{\mathbf{q}'}\right).$$

In both proofs, we follow the method from Dodson [2].

Proof of Proposition 3. By the rank equation, the solution curves to the equations $\mathbf{q}A = \mathbf{p}$ are $(m-1)n$ dimensional affine spaces over $\mathcal{L}$. We begin by calculating the number of affine spaces which pass through the unit ball. First, note that if there is a solution to the equation $\mathbf{q}A = \mathbf{p}$ with $A \in I^{mn}$, then

$$\|\mathbf{p}\|_{\infty} = \|\mathbf{q}A\|_{\infty} \leq \|\mathbf{q}\|_{\infty}\|A\|_{\infty} < \|\mathbf{q}\|_{\infty}, \tag{4}$$

so certainly, the condition $\|\mathbf{p}\|_{\infty} < \|\mathbf{q}\|_{\infty}$ is necessary. We claim that it is also sufficient.

For this, it suffices to find a solution $A \in I^{mn}$ which satisfies the equation. Suppose that $\|\mathbf{p}\|_{\infty} < \|\mathbf{q}\|_{\infty}$. We assume without loss of generality that $\|\mathbf{q}\|_{\infty} = \|q_1\|$. Now,

$$\mathbf{q}A = \mathbf{q}\begin{pmatrix} p_1/q_1 & \cdots & p_n/q_1 \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} = \mathbf{p} \tag{5}$$

and $A \in I^{mn}$.

As in Dodson [2], we consider the simplest non-trivial case where $\mathbf{q} = (q_1, q_2)$ and $\mathbf{p} = p$ and subsequently extend this to the general case. In this case, the solution curves to the equations $\mathbf{q}A = p$ define $\|\mathbf{q}\|_{\infty}$ affine 1-dimensional spaces in I^2. These partition I^2 into $\|\mathbf{q}\|_{\infty}$ strips, $\tilde{S}_i$ say, defined by inequalities $\|\mathbf{q}A - p\| < 1$. The measure of each such strip may be calculated using a characterisation of a translation invariant measure due to Mahler (see [5]), which implies that the measure of a parallelogram is $1/\det(w_1, w_2)$, where w_1 and w_2 are the spanning vectors. Since the distance between each affine 1-space is $1/\|\mathbf{q}\|_{\infty}$, the solution curves partition I^2 into sets of the same size, $\mu(\tilde{S}_i) = 1/\|\mathbf{q}\|_{\infty}$. By the same characterization, we

find that around each solution curve we have a component, B_i say, of the set $B_{\mathbf{q}}$ of measure $\psi(\mathbf{q})/\left\|\mathbf{q}\right\|_\infty$. Hence

$$\mu\left(B_{\mathbf{q}}\right) = \frac{\mu\left(B_{\mathbf{q}}\right)}{\mu(I^2)} = \frac{\mu\left(\cup B_i\right)}{\mu\left(\cup \tilde{S}_i\right)} = \frac{\mu(B_i)}{\mu(\tilde{S}_i)} = \frac{\psi(\left\|\mathbf{q}\right\|_\infty)/\left\|\mathbf{q}\right\|_\infty}{1/\left\|\mathbf{q}\right\|_\infty} = \psi(\left\|\mathbf{q}\right\|_\infty). \quad (6)$$

To obtain the proposition for general $m, n \in \mathbb{N}$, consider n copies of the span of $\mathbf{q}$ and apply the above argument to resulting prisms in I^{mn}. This implies the proposition. □

Proof of Proposition 4. Again, we consider the simplest non-trivial case, $m = 2, n = 1$. Let $\mathbf{q}, \mathbf{q}' \in \mathbb{F}[X]^2$ be linearly independent. We calculate the number of intersections between the solution curves to the equations $\mathbf{q}A = p$ and the equations $\mathbf{q}'A = p'$, where p, p' runs over the possible values. This amounts to solving the system

$$\begin{pmatrix} q_1 & q_2 \\ q_1' & q_2' \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} p \\ p' \end{pmatrix}, \quad \left\|p\right\|_\infty < \left\|\mathbf{q}\right\|_\infty, \left\|p'\right\|_\infty < \left\|\mathbf{q}'\right\|_\infty.$$

There are exactly $\left\|\det\left(\begin{smallmatrix} q_1 & q_2 \\ q_1' & q_2' \end{smallmatrix}\right)\right\|$ such solutions. To each such solution, we may assign a parallelogram defined by the inequality

$$\max\{\left\|\mathbf{q}A - p\right\|, \left\|\mathbf{q}'A - p\right\|\} < 1$$

The parallelogram is seen to be of measure $1/\left\|\det\left(\begin{smallmatrix} q_1 & q_2 \\ q_1' & q_2' \end{smallmatrix}\right)\right\|$, and the parallelograms are mutually disjoint.

To show that these parallelograms partition I^2, it remains to be shown that each of the parallelograms defined above is a proper subset of I^2. But this is the case, since any parallelogram may be written as

$$\left\{x \in \mathcal{L}^2 : x = \hat{q}_1 t_1 + \hat{q}_2 t_2 + p, t_1, t_2 \in I\right\}$$

for some $\hat{q}_1, \hat{q}_2 \in \mathcal{L}^2$. Clearly,

$$\left\{x \in \mathcal{L}^2 : x = \hat{q}_1 t_1 + \hat{q}_2 t_2 + p, t_1, t_2 \in I\right\} \subseteq B\left(p, \max\left(\left\|\hat{q}_1\right\|_\infty, \left\|\hat{q}_2\right\|_\infty\right)\right),$$

so by the ultrametric property, the parallelogram is either fully contained in I^2 or disjoint with I^2. Since the parallelograms bounded by the solution curves are disjoint, there can be no more than the required number.

Furthermore, around each intersection point, there is another parallelogram of measure $\psi(\mathbf{q})\psi(\mathbf{q}')/\left\|\det\left(\begin{smallmatrix} q_1 & q_2 \\ q_1' & q_2' \end{smallmatrix}\right)\right\|$, constituting a part of $B_{\mathbf{q}} \cap B_{\mathbf{q}'}$ whenever it is a subset of I^2.

With the above tools, we may apply a proportionality argument analogous to (6) to obtain the proposition in this case. For the general case, we consider n copies of the span of $\mathbf{q}$ and $\mathbf{q}'$ and apply the above to the mn dimensional prisms to obtain the proposition. $\square$

We are now ready to prove the main theorem.

Proof of Theorem 2. The final ingredient in the proof is Lemma 10 in Sprindžuk [10].

Let $f_{\mathbf{q}}(A)$ be the characteristic function of $B_{\mathbf{q}}$, $f_{\mathbf{q}} = \psi(\|\mathbf{q}\|)^n$ and let $\tau(\mathbf{q}) = \psi(\mathbf{q})^n d(\mathbf{q})$, where $d(\mathbf{q})$ denotes the number of common divisors in $\mathbb{F}[X]$ of the coordinates of $\mathbf{q}$. Clearly, by Proposition 3 and Proposition 4 for $s < t$,

$$\int \left(\sum_{k^s < \|\mathbf{q}\|_\infty \le k^t} f_{\mathbf{q}}(A) - \sum_{k^s < \|\mathbf{q}\|_\infty \le k^t} f_{\mathbf{q}} \right)^2 dA \ll \sum_{k^s < \|\mathbf{q}\|_\infty \le k^t} \tau_{\mathbf{q}},$$

as we only get contributions from the diagonal and elements that corresponding to pairs of parallel $\mathbf{q}$'s. By Lemma 10 in Sprindžuk [10], we then have for almost every A,

$$N(Q,A) = \sum_{\|\mathbf{q}\|_\infty \le k^Q} f_{\mathbf{q}}(A) = \sum_{\|\mathbf{q}\|_\infty \le k^Q} f_{\mathbf{q}} + O\left(T(Q)^{1/2} \log^{3/2+\epsilon} T(Q)\right), \quad (7)$$

where $T(Q) = \sum_{\|\mathbf{q}\|_\infty \le k^Q} \tau(\mathbf{q})$. We need to prove that the right hand side is dominated by the first term.

We begin with this term. By formula (1.4) in Kristensen [3],

$$\sum_{\|\mathbf{q}\|_\infty \le k^Q} f_{\mathbf{q}} = \sum_{r=0}^{Q} \sum_{\|\mathbf{q}\|_\infty = k^r} \psi(k^r)^n = m(k-1)k^{m-1} \sum_{r=0}^{Q} k^{rm} \psi(k^r)^n = \Phi(Q).$$

Thus we need only worry about the error term $T(Q)$. Clearly, it suffices to prove that

$$T(Q) = O(\Phi(Q)).$$

We first observe that by denoting $\mathbf{q} = (q_1, \ldots, q_m)$ and again applying (1.4) from Kristensen [3],

$$\#\{\mathbf{q} \in f[X]^m \colon \|\mathbf{q}\|_\infty = k^r\} = m(k-1)k^{m-1+rm},$$

which gives the number of $\mathbf{q}$ of given height k^r, we immediately obtain

$$\begin{aligned}
T(Q) &= \sum_{\|\mathbf{q}\|_\infty \le k^Q} \psi(\|\mathbf{q}\|_\infty)^n \sum_{d|(q_1,\ldots,q_m)} 1 \\
&\ll \sum_{r=0}^{Q} \sum_{\alpha=0}^{r} \sum_{\substack{\|\mathbf{q}\|_\infty = k^r \\ \mathrm{GCD}(q_1,\ldots,q_m)=a=k^\alpha}} \psi(\|\mathbf{q}\|_\infty)^n \sum_{d|a} 1 \\
&\ll \sum_{r=0}^{Q} \psi(k^r)^n \sum_{\alpha=0}^{r} \sum_{\substack{\|\mathbf{v}\|_\infty = k^{r-\alpha} \\ \mathrm{GCD}(v_1,\ldots,v_m)=1}} 1 \\
&\ll \sum_{r=0}^{Q} \psi(k^r)^n \sum_{\alpha=0}^{r} m(k-1)k^{m-1}k^{(r-\alpha)m} \\
&\ll m(k-1)k^{m-1} \sum_{r=0}^{Q} \psi(k^r)^n k^{rm} \sum_{\alpha=0}^{r} k^{-\alpha m} \\
&\ll m(k-1)k^{m-1} \sum_{r=0}^{Q} \psi(k^r)^n k^{rm} \ll \Phi(Q),
\end{aligned}$$

as required. □

3 Acknowledgements

We thank the referee for some helpful comments. Research partially funded by EPSRC grant no. GR/N02832/01 with additional support from INTAS grant no. 001–429. SK is a William Gordon Seggie Brown Fellow.

References

[1] B. de Mathan, Approximations diophantiennes dans un corps local, *Bull. Soc. Math. France Suppl. Mém.*, **21** (1970), 1-93.

[2] M. M. Dodson, Geometric and probabilistic ideas in the metric theory of Diophantine approximations, *Uspekhi Mat. Nauk*, **48** (1993), no. 5(293), 77-106.

[3] S. Kristensen, On well-approximable matrices over a field of formal series, *Math. Proc. Cambridge Philos. Soc.*, **135** (2003), no. 2, 255-268.

[4] A. Lasjaunias, A survey of Diophantine approximation in fields of power series, *Monatsh. Math.*, **130** (2000), no. 3, 211-229.

[5] Kurt Mahler, An analogue to Minkowski's geometry of numbers in a field of series, *Ann. of Math. (2)*, **42** (1941), 488-522.

[6] H. Niederreiter and M. Vielhaber, Linear complexity profiles: Hausdorff dimension for almost perfect profiles and measures for general profiles, *J. Complexity*, **13** (1997), 353-383.

[7] W. M. Schmidt, A metrical theorem in Diophantine approximation, *Canad. J. Math.*, **12** (1960), 619-631.

[8] W. M. Schmidt, Metrical theorems on fractional parts of sequences, *Trans. Amer. Math. Soc.*, **110** (1964), 493-518.

[9] W. M. Schmidt, On continued fractions and Diophantine approximation in power series fields, *Acta Arith.*, **95** (2000), no. 2, 139-166.

[10] V. G. Sprindžuk, *Metric theory of Diophantine approximations*, V. H. Winston & Sons, Washington, D.C. (1979).